(12) UK Patent Application (19) GB (11) 2 352 861 (13) A

(43) Date of A Publication 07.02.2001

(21) Application No 9918246.1

(22) Date of Filing 04.08.1999

(71) Applicant(s)
International Computers Limited
(Incorporated in the United Kingdom)
26 Finsbury Square, LONDON, EC2A 1SL,
United Kingdom

(72) Inventor(s)
Ed Wilson

(74) Agent and/or Address for Service
Susan Mary Dupuy
Intellectual Property Department,
International Computers Limited, STEVENAGE,
Hertfordshire, SG1 2DY, United Kingdom

(51) INT CL^7
G07F 7/10

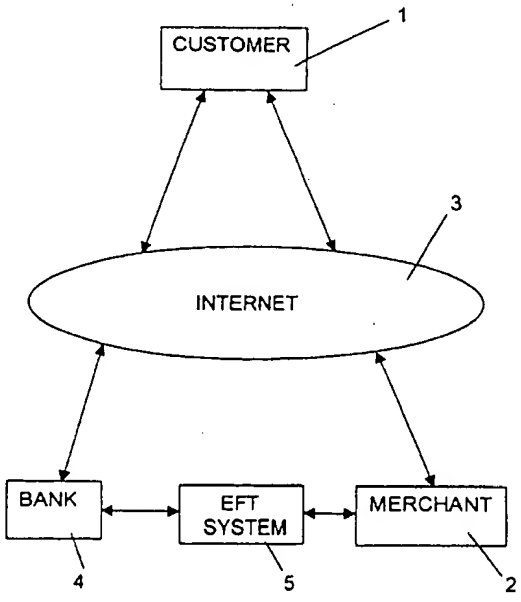
(52) UK CL (Edition S)
G4V VAK
G4T TBX

(56) Documents Cited
EP 0747867 A1 **WO 98/30985 A2** **WO 98/13795 A1**

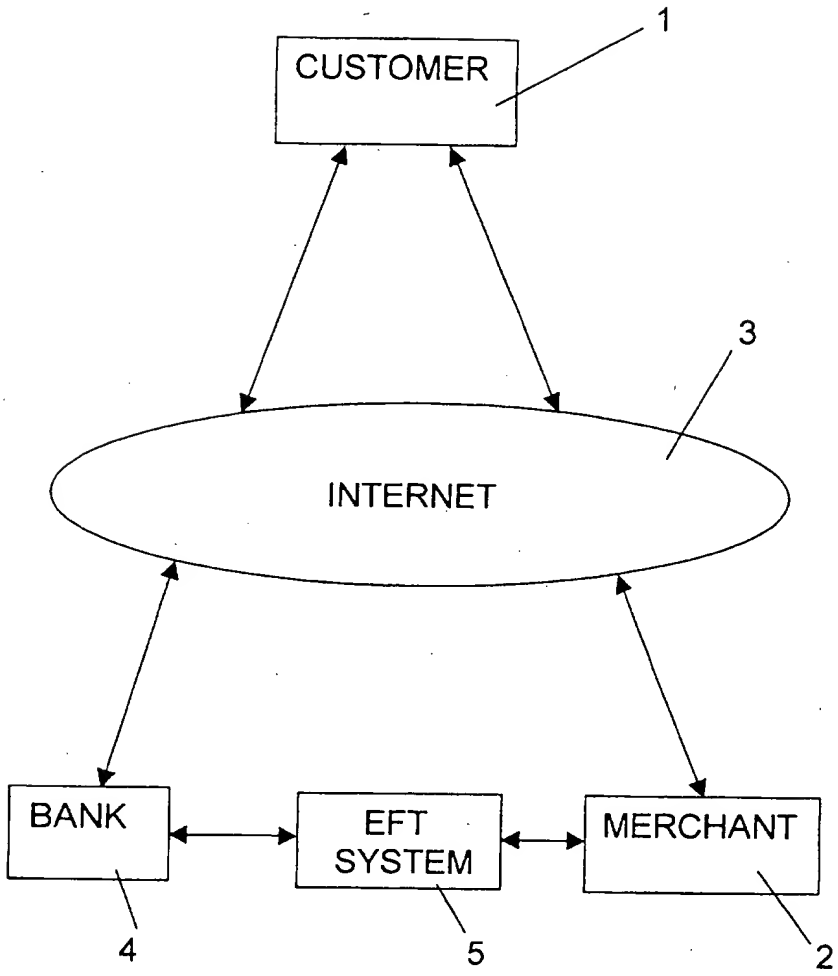
(58) Field of Search
UK CL (Edition Q) **G4T TBX , G4V VAK**
INT CL^6 **G07F 7/08 7/10**

(54) Abstract Title
Payment transaction system

(57) A payment transaction system particularly, but not exclusively, for the purchase by a customer (1) of goods offered by a merchant (2) on the Internet (3), which prevents unlimited access by the merchant (2) to a customer's account. Instead of supplying, for example, credit card details which would permit an unscrupulous merchant to extract more of the customer's money than intended, an identifier for a specific quantity of money (the cost of the goods) is used. The identifier is generated by the customer's bank (4), for example, in response to a specific request by the customer, transmitted by the bank to the customer and supplied to the merchant instead of a credit card number. The merchant employs the identifier, in a similar way to a credit card number, in order to obtain payment using an Electronic Funds Transfer (EFT) system (5). The identifier represents, but does not include, details of the account on which it is to be drawn, the value of the order and a set of time rules. The time rules, for example, mean that the identifier must be used within a predetermined time interval, such as 24 hours after allocation, and which mean that once the rules are invoked the identifier is invalidated, so that it can be used only once. The identifier does not allow a merchant access to the account. Thus, while the customer may not receive the ordered goods, they can be paid for only once.



GB 2 352 861 A


CUSTOMER
1
3
INTERNET
BANK
EFT
SYSTEM
MERCHANT
4
5
2

PAYMENT TRANSACTION SYSTEM

This invention relates to a payment transaction system and a payment method, and in particular, but not exclusively, to a payment transaction system for use on world-wide networks, e.g. the Internet.

Since it is perceived as dangerous, and sometimes actually is, to give credit card details over a World Wide Web link, or even over the telephone, various transaction schemes have been proposed to maintain the security of a credit card number when it is transferred from one point to another over the Internet. However, if those receiving the number are incompetent or dishonest, the fact that the number was secure during transfer does not prevent subsequent misuse of it. Other prior transaction schemes are such that credit card numbers are not transmitted over the Internet, but require both a vendor and a buyer to be registered with a trusted organisation. The vendors and buyers have respective accounts with the organisation and may be assigned unique PINs that they use to identify themselves during transactions, which can comprise a number of email exchanges. As well as having an email address, each account with the organisation has associated with it a real-world account and methods to transfer funds between the accounts. A currency for such funds transfer may be predefined. The transaction process for a buyer with a credit card account as the real-world account, comprises the buyer initiating a purchase and giving their PIN number to the vendor. The vendor emails this PIN number together with their own PIN number and a description of the purchase to the organisation, which automatically sends an email to the buyer for confirmation. The buyer sends confirmation to the organisation, by return email, and the organisation uses existing secure financial networks to process the credit card transaction. Once this is completed, the vendor is sent an authorisation number which enables the vendor to receive the appropriate funds.

Other proposed schemes involve electronic cash or electronic cheques, the latter being issued by trusted parties, such as banks, and, typically, validated by a signature which is encrypted using a public key algorithm, such as RSA. Electronic cash systems have been proposed which involve tokens of fixed value, that is electronic coins, which are spent by transferring the tokens. Fixed value tokens, however, involve a "change" problem if the buyer does not have the correct

denominations of coins to make the exact price, and various proposals have been made to accommodate the issuance of "change". The issuer of such tokens must be trusted organisations, such as banks, and the tokens will generally include the name of the server issuing them, a serial number for the token and a value for the token, as well as being signed by the server's private key for security purposes. Double spending tests are commonly employed to ensure that a token can be spent only once. An additional problem is that the merchant (vendor) must have the agreements and the processes to recognise, process and bank the particular electronic currency.

As will be appreciated, these tokens are generally obtained from the server concerned in advance of any particular purchase. This is the case where they are used for the payment of services obtained on the Internet and large quantities of low-value tokens may be involved. In PCT/GB97/03116 (WO 98/22915) there is disclosed a system involving purchase of a carnet of tokens from a payment service using a public key encrypted credit card number sent to the service. The tokens are encrypted with the public key algorithm and returned to the purchaser together with a key that is unique to the purchaser. When a merchant requests payment, one or more tokens are issued to them over the Internet by the purchaser. The merchant has to subsequently contact the payment service in a token authentication process, and the payment service, after authenticating the token, updates the merchant's account record.

Whilst the prior proposals are undoubtedly suitable for specific purposes, they are generally quite complicated and involve, for example, the use of encryption, change problems and/or numerous emails.

The present invention aims to provide a relatively simple payment transaction process, which is particularly, but not exclusively, applicable to the purchase by individuals of goods offered by merchants on the Internet and which ensures that whilst the merchant may take the money and not supply the goods, the money can only be taken once.

According to one aspect of the present invention there is provided a method of payment for goods/services to be purchased by a customer from a merchant at a predetermined cost, the customer having an account with a financial service provider from which the cost is to be

debited, the account having a number and being PIN or password protected, including the steps of the customer contacting the financial service provider to obtain a payment identifier for use by the merchant, the payment identifier representing, but not including, the account number, the predetermined cost and time for payment rules, and the PIN or password; the customer advising the merchant of the identifier; the merchant employing the identifier in an electronic funds transfer system whereby to request payment; and the request being honoured by the financial service provider if the payment requested is in accordance with the predetermined cost and in accordance with the time for payment rules.

According to another aspect of the present invention there is provided a payment transaction system including a financial service provider, for the issuance of payment identifiers to first persons wishing to pay second persons for goods/services provided at a predetermined cost to the first persons in a manner which restricts the liability of the first persons, the first persons having accounts with the financial service provider from which the cost is to be debited, which accounts have numbers and are PIN or password protected, wherein the payment identifiers represent, but do not include, details of the respective predetermined cost and respective time for payment rules, the number of the account to be debited, and the PIN or password; and an electronic funds transfer system with which the second persons employ the payment identifiers supplied to them by the first persons whereby to request payment, the financial service provider honouring a said request for payment if it is in accordance with the respective predetermined cost and the respective time for payment rules.

Embodiments of the invention will now be described with reference to the accompanying drawing which illustrates a payment transaction system highly schematically.

Apart from the role of the individual customer, the taker of responsibility, there are two other significant roles in a payment transaction, namely the trusted organisation and the unknown quantity. The trusted organisation is the bank, building society or other financial organisation to which the customer has entrusted his money. The unknown quantity is the person or organisation (merchant) to which money is to be paid. Many of these are trustworthy in objective terms, but there can be those which are untrustworthy and may use the customer's credit card

number, for example, for other than the intended purchase. It can be some time before the customer realises this and closes the account or takes other action in association with the bank to prevent further such use.

Instead of supplying a merchant with a number which gives a merchant open access to the customer's account, the invention proposes that an identifier for a specific quantity of money is supplied. Whilst that quantity might be lost to an unscrupulous merchant, who fails to supply the goods, access to other funds is prevented.

The identifier is a number, sent along all the same secure lines as credit card numbers are now, between customers, merchants and banks, which entitles the bearer to a defined quantity of money in a specified currency from the customer's bank or credit account, but does not allow access to the whole bank or credit account. The customer acquires this number from the trusted organisation, supplies it to the unknown quantity (merchant) which can then make that charge and no more for the service or goods the customer wishes to purchase. The service or goods may not be supplied, but they are paid for only once. Hence, the customer's liability is limited.

It is proposed that the trusted organisation will offer a payment transaction system involving such identifiers to its customers. In the case of a transaction involving the Internet, this will involve a download of software to a customer PC and a secure connection service. A customer who wants to make a purchase will need to supply credit card, debit card or other agreed details, plus a PIN or password, to the trusted organisation (bank). In addition, the amount of money must be specified as a number and a currency. If all the details are accepted, the customer receives the identifier (code) which is sent to and used by the merchant as if it were a credit card number in a request for x US dollars, y German marks etc. The identifier is associated with a set of rules, actioned by the bank's system. The rules state that the bearer of the identifier is entitled to request a specified amount of money within a given time period. This could, for example, be set to expire 24, 48 or more hours after the code is allocated, depending on the bank's processes. The rules invalidate the identifier as soon as they have been invoked, so that the money can only be requested once, or invalidate it after the expiry period, whichever comes first. Extensions to the system might produce rules which can be invoked once a month for repeated payments, but

changes would only be possible with approval by the customer. The availability of repeat requests would be dictated by the rules, not by any information sent by the merchant.

The identifier is a token for a specified quantity of money and has time rules attached. The identifier has the following attributes, only the first of which is visible to the merchant:

- an identifying code, which is the same kind of string as is used for a credit card number, although changes to this may be needed in the future, for example use of more than 16 digits or an alphanumeric string rather than just numbers.

- the account on which it is to be drawn, for example a credit card account, a general bank account or even an account specifically designed for use with identifiers. Access to the account would, for example, need an account or card number and a PIN or password for verification.

- the value of the order, specified as a number and currency. The actual amount taken from an account will depend on conversion rates at the moment of transfer, but the value of the order, for example 500 Hong Kong dollars, is the maximum that would be paid.

- time rules, the simplest example of which is a date and time at which the identifier becomes effective, normally the moment of issue, and a date and time at which it expires if it has not been redeemed. The transaction might, for example, have to be completed in two days. More complex rules could be used. A delayed effective date so that it becomes effective on a recipient's birthday, or a repeating formula which allows an agreed sum of money to be claimed once between the first and third of each month, for example.

In the following, the trusted organisation or body offering such a payment transaction system is referred to as a bank, although other types of financial organisations could offer such products. Quite which products are offered, and the rules for issue and redemption of the identifier, would be up to the bank. For example, can an identifier be issued if there is too little in the account? A

trusted third party, such as the Post Office, could offer the identifier service on behalf of one or more clients.

An identifier may be requested in a variety of ways, for example by telephone, letter or personal attendance at a sales counter, although the most obvious means of transmission is the Internet, as will be seen from the example set out below.

The customer will need software to request the appropriate information and handle transmission (secure) to and from the bank. This can be a small program (applet) provided as part of an electronic banking service. The program would be installed in such a way that it would be invoked from the customer's browser (World Wide Web interface program) and communicate with the bank by means of a standard secure protocol (such as HTTPS). The bank will need new software to process requests for identifiers, but the payment side can be handled largely through existing Electronic Funds Transfer (EFT) systems, which may or may not involve the Internet. The merchant needs no special software since the identifier can be treated as if it were a credit card number.

Consider the following example and the accompanying drawing. A customer 1 wishes to buy a shirt from a merchant 2 advertising on the Internet 3. The customer has had no previous dealings with the merchant, who is based overseas, and is reluctant to send his credit card details over the Internet. The customer's bank 4, however, offers a payment transaction system. Hence, the transaction can be completed quickly over the Internet, and in the worst case scenario, the customer will pay once for the shirt but not receive it. The steps in the transaction are indicated in Table 1.

Customer	Bank	Merchant
Calls up identifier applet from browser.		
Enters account number, sum of money (cost of goods), and currency. The applet sends this information to the bank over the Internet using secure channels. Information transferred to bank: account number, sum to pay (number/currency)	Software requests confirmation, prompting with financial details (cost of goods) and requesting PIN. Information transferred to customer: sum to pay	
Sends PIN Information transferred to bank: PIN	If customer request conforms to bank's rules, generates identifier, records details, sends identifier to customer. Information transferred to customer: Identifier (without any details of customer's account)	

Fills in order form for shirt, entering identifier instead of credit card number. Sends to Merchant. Information transferred to merchant: Identifier		Submits details of payment required and identifier through EFT System 5. Information supplied to bank or EFT system: Identifier
	Honours the identifier if before expiry date and right amount requested. Transfers amount from customer's account.	Receives confirmation payment has been made and despatches shirt.
Waits for shirt.		

Table 1

Notes

(1) Calling up the identifier applet results in a window opening over the page the customer was reading, possibly that containing an advertisement and/or order form for the shirt in question.

(2) When the bank requests the PIN it does not repeat the account number, so that the account number and the PIN are never part of the same transaction.

(3) Sending the PIN is an Internet interaction performed in the applet window.

(4) The identifier is used for the EFT system as if it were a credit card number.

(5) Once the appropriate amount has been transferred from the customer's account, the identifier is spent and the corresponding number cannot be used again.

(6) At any stage until the customer supplies the identifier to the merchant, the customer can cancel and abort the whole transaction. Even if the bank has supplied the identifier to the customer, all the latter has to do is fail to use it until it expires and nothing will be taken from the customer's account.

(7) Any charges for the service itself will be a matter for agreement between the bank and its customers.

(8) An audit trail, including the merchant's bank details, can be recorded by the bank and a subset of this information can be included in the customer's statement.

Whilst the invention has been described with reference to the purchase of goods offered and ordered over the Internet, it will be appreciated that it is equally applicable to other payment scenarios, for example the purchase of goods by mail order, where hitherto credit card details, for example, are supplied that an unscrupulous merchant could use to extract further monies from a customer. The identifier limits the merchant to receiving a maximum amount and typically only once, due to the time rules associated with the identifier. Unlimited access to the customer's account is prevented since the merchant does not have access to any real account number or PIN. In other words, no banking details relating to the customer are supplied to the merchant, and the identifier specifies a maximum amount the merchant can receive. The identifier represents, but does not include, the account number, the cost and time for payment rules and the PIN or password. In effect, there is a firewall between a merchant and a customer's permanent account with a bank. The merchant is given an "access token" for a specified sum, but only the bank can identify the permanent account from the "access token". With regard to the purchase of goods over the Internet, it should be noted that with the above-described system, a purchase need take

hardly any longer than a conventional credit card payment with the issuance of the identifier automated. With good telephone lines, it should take a matter of seconds.

CLAIMS

1. A method of payment for goods/services to be purchased by a customer from a merchant at a predetermined cost, the customer having an account with a financial service provider from which the cost is to be debited, the account having a number and being PIN or password protected, including the steps of the customer contacting the financial service provider to obtain a payment identifier for use by the merchant, the payment identifier representing, but not including, the account number, the predetermined cost and time for payment rules, and the PIN or password; the customer advising the merchant of the identifier; the merchant employing the identifier in an electronic funds transfer system whereby to request payment; and the request being honoured by the financial service provider if the payment requested is in accordance with the predetermined cost and in accordance with the time for payment rules.

2. A method as claimed in claim 1, wherein the time for payment rules are such that a single payment is involved and the identifier is rendered invalid at the end of a predetermined time interval or when the time for payment rules are invoked, whichever occurs first.

3. A method as claimed in claim 1, wherein the time for payment rules are such that multiple payments, each at a predetermined time with reference to a previous payment or at a predetermined day of a calendar month, are involved, and wherein the identifier is only valid for a predetermined time interval for each payment.

4. A method as claimed in claim 2, wherein the start of the predetermined time interval is selected by the customer.

5. A method as claimed in claim 1, wherein the step of the customer contacting the financial service provider includes the steps of the customer advising the financial service provider of the number of the account, the predetermined cost and the currency for payment; the financial service provider requesting confirmation by advising the customer of the predetermined cost and the currency and requesting the PIN or password; the customer

providing the PIN or password to the financial service provider; and the financial service provider generating the identifier and supplying it to the customer.

6. A payment transaction system including a financial service provider, for the issuance of payment identifiers to first persons wishing to pay second persons for goods/services provided at a predetermined cost to the first persons in a manner which restricts the liability of the first persons, the first persons having accounts with a financial service provider from which the cost is to be debited, which accounts have numbers and are PIN or password protected, wherein the payment identifiers represent, but do not include, details of the respective predetermined cost and respective time for payment rules, the number of the account to be debited, and the PIN or password; and an electronic funds transfer system with which the second persons employ the payment identifiers supplied to them by the first persons whereby to request payment, the financial service provider honouring a said request for payment if it is in accordance with the respective predetermined cost and the respective time for payment rules.

7. A payment transaction system as claimed in claim 6, wherein the time for payment rules are such that a single payment is involved and the identifier is rendered invalid at the end of a predetermined time interval or when the time for payment rules are invoked, whichever occurs first.

8. A payment transaction system as claimed in claim 6, wherein the time for payment rules are such that multiple payments, each at a predetermined time with reference to a previous payment or at a predetermined day of a calendar month, are involved, and wherein the identifier is only valid for a predetermined time interval for each payment.

9. A payment transaction system as claimed in any one of the claims 6 to 8 and wherein communications between the first persons, the second persons and the financial service provider take place over the Internet.

10. A payment transaction system substantially as herein described with reference to and as illustrated in the accompanying drawing.

11. A method of payment for goods/services substantially as herein described with reference to and as illustrated in the accompanying drawing.

The Patent Office

14.

INVESTOR IN PEOPLE

Application No: GB 9918246.1 **Examiner:** Dave McMunn
Claims searched: 1-11 **Date of search:** 22 November 1999

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.Q): G4V (VAK). G4T (TBX).

Int Cl (Ed.6): G07F 7/08, 7/10.

Other: -

Documents considered to be relevant:

Category	Identity of document and relevant passage	Relevant to claims
Y	EP 0,747,867 A1 (FRANCE TELECOM). See Fig 1	1,2,5-7,9
X	WO 98/30985 A2 (KAMIL). See Figs 1 & 5	1,2,5-7,9
Y	WO 98/13795 A1 (& GB2317790) (BILLINGSLEY). Note time validity	1,2,5-7,9

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.